Cybersecurity Lessons from Safety

Experts have long advocated for the alignment of cybersecurity and safety to ensure overlapping protections. A number of methods, from protection layering to analytical methods, provide guidance on how to achieve this.

James R. Koelsch
Apr 10th, 2020

Cybersecurity needs to be thoroughly ingrained in manufacturing operations, much like safety has generally become today. That's why many cybersecurity advocates have long proposed that automation professionals exploit some of the similarities between cybersecurity and safety. The idea is to adapt best practices from safety to defend against cyberattacks.

“There are decades of experience in applying safety standards and best practices,” explains Luis Duran, global product manager for safety systems at ABB. “And that experience can be beneficial for establishing new best practices for dealing with a different problem like cybersecurity.”

“Safety practices are already more widely understood and ingrained than cybersecurity practices,” adds Alexandre Peixoto, product manager for DeltaV cybersecurity at Emerson Automation Solutions. “So, safety comparisons help a lot with cybersecurity acceptance.”

These comparisons are possible because the two disciplines are alike in important ways. Fundamentally, both are aimed at managing risks that never completely go away. Just as carelessness or unforeseen circumstances can foil well-devised safety practices, a concerted effort undertaken by a skilled attacker will eventually get past even the best cyber defenses.

The general security strategy from this vantage point is to mitigate risk by erecting several layers of defense, each aimed at preventing incidents from occurring or containing damage if defenses are eventually breached. “An effective cybersecurity posture for industrial control systems is based on a defense-in-depth strategy, which is much like the layers-of-protection analysis for safety systems,” says Peixoto.

This means that, like safety, cybersecurity must be designed into control networks from the outset. “Too often, manufacturing organizations add cybersecurity defenses later,” observes Peixoto. “It’s more expensive and rarely as effective as building cybersecurity into the project.”

The implementation of safety and cybersecurity, moreover, must go beyond technical solutions. “Both also require behavioral and cultural change,” explains Peixoto. “A deeply rooted understanding of the ‘why’ and ‘how’ among everyone in the company—from management to plant personnel—is critical to driving meaningful behavioral change in cybersecurity.”

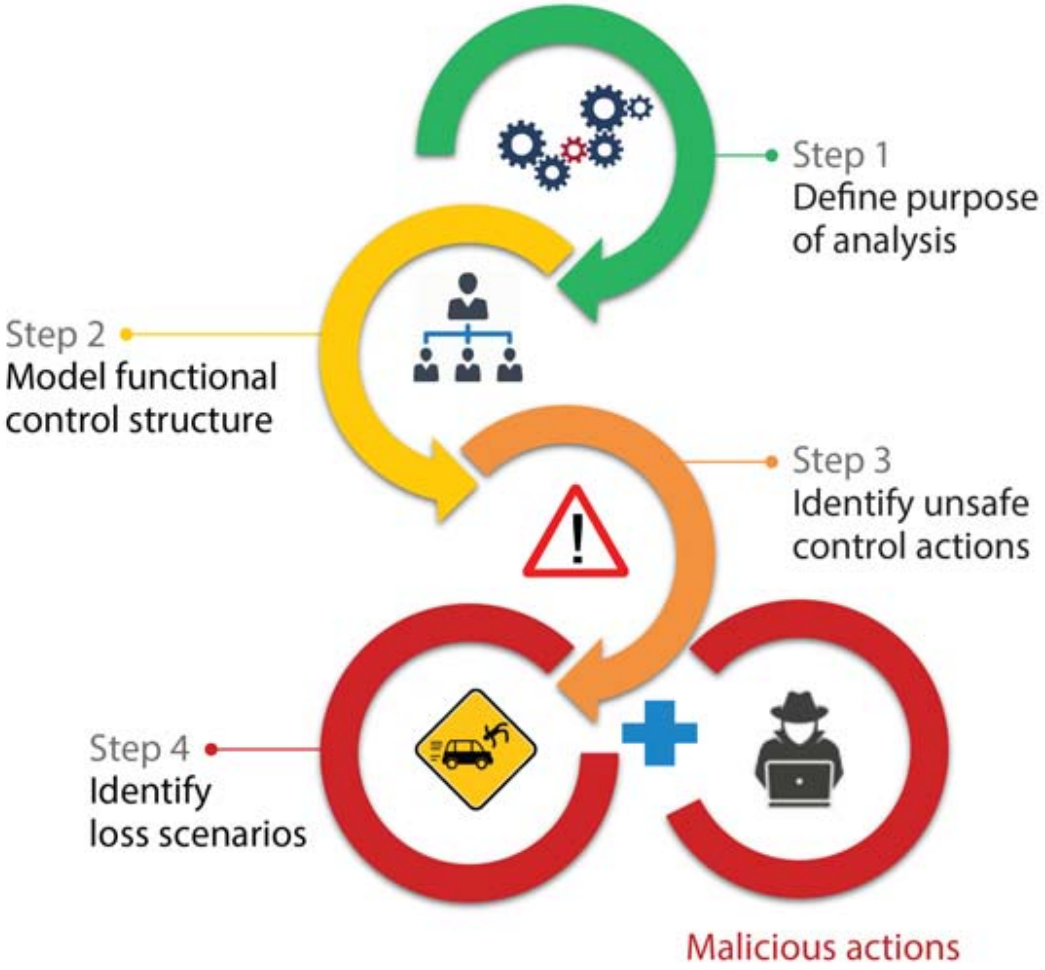
Manufacturers must, therefore, support this strategy by developing policies and procedures and conducting periodic training, as they do for their safety programs. “It’s paramount that the asset owner has policies and procedures

defined and enforced so that secure operating procedures are clear and known by everyone in the plant," stresses Peixoto.

For both safety and cybersecurity, however, risk mitigation is not really a destination that is ever reached. Instead, Duran at ABB calls it a journey, one that requires continued vigilance, preparedness, and action suited to each stage of each asset's lifecycle. "Users should periodically reassess established practices and determine whether or not they are working," he says.

Called cybersafety, the four-step method diagrammed here describes how to analyze the cybersecurity of manufacturing operations. MIT researchers developed this method by adapting a model for analyzing accidents to apply it to cyberattacks on cyber-physical systems. Courtesy of the MIT.

Similar but different



Despite these similarities, the idea of using safety as a model for cybersecurity in industrial automation has not yet been widely implemented in industry. The

reasons tend to revolve around some crucial differences between the two disciplines.

First is the lack of regulations mandating cybersecurity. Whereas regulatory bodies have been requiring and enforcing various safety standards in industry for decades now, cybersecurity standards for industrial automation are not only relatively new, but also tend to be voluntary. Hence, their adoption has mostly depended on the manufacturing organization and its perception of the risk of not implementing them.

Recently, however, Dr. Alexander Horch, vice president of research and development and product management at the Hima Group, has noticed a welcome trend. “Companies in the process industry are increasingly recognizing the importance of safety and security standards for the safety and economic viability of their plants,” he says. The main standards the process industry follows are IEC 61508 and IEC 61511 for safety, and the IEC 62443 cybersecurity standard.

Horch believes that complying with such standards is as important to defending against cyberattacks as it has been for improving safety. “For safety, it has worked brilliantly for 50 years,” he says. “For security, though, the standard is necessary, but not sufficient. Since the threat is constantly changing, security must also be constantly checked, not only for function, but also for effectiveness.”

This constantly changing landscape is perhaps the most crucial way that cybersecurity differs from safety. “In safety, we strive to understand the physical process and how various failures in the operation or design could create dangerous conditions,” explains Duran at ABB. “Then, we design mitigations. We generally do not expect new failure modes to materialize.

With cybersecurity, the situation is different. “We have to deal with malicious intent, which is very unpredictable,” says Donovan Tindill, a cybersecurity expert at Honeywell Connected Enterprise. “It’s more about the nature of the threat. What are the capabilities and motivations of the attackers, and how do they compare to the cybersecurity to protect the control system?”

In addition to these factors, the strategies used by the attackers are also constantly evolving, making it difficult to predict the likelihood of success or failure of any attack. Consequently, process and security designers generally cannot rely on a body of statistics similar to the data on equipment failure that is available for safety engineering.

Another factor contributing to the unpredictability of cyberattacks is the constant evolution of technology. “Each time a new technology is invented—like cloud computing, mobile devices, and quantum computing—it introduces a new set of cybersecurity challenges,” notes Tindill. New controls for protection and detection must be developed and integrated into business processes and technology.

The unpredictability of cyberattacks means that designers are really guarding against different kinds of error. “Functional safety essentially deals with random errors, while security attacks are more likely to be systematic errors due to weaknesses,” says Horch.

These fundamental differences lead to different implementation strategies. “Safety is usually done once, and the effectiveness of the measures taken is checked regularly,” he says. “Security has to be done constantly, because the risk is constantly changing.”

“You need to keep evaluating the threat landscape, as well as the probing indicators,” adds Duran at ABB. “This means active monitoring of edge firewalls and system networks. It also means active involvement with the industrial control system cybersecurity community to share information and learn about trends so that you can prepare and adapt.”

Professor Stuart Madnick (left) and graduate student Shaharyar Khan, working with Professor James Kirtley (not shown), found several vulnerabilities when they applied MIT's cybersafety method in this small power plant. The plant is susceptible to cyberattacks because it uses software, rather than mechanical devices, to keep the turbines from exceeding their control limits. Photo credit: Stuart Darsch

A new approach

Taking these key differences into account, researchers continue to leverage the similarities between safety and cybersecurity to apply lessons learned. One result of this search has been cybersafety, a top-down analytical method developed at the Massachusetts Institute of Technology (MIT). This method is an adaptation of a model developed by Nancy Levering at MIT 15 years ago for analyzing accidents of all kinds.

This new cybersafety method has four steps, according to Stuart Madnick, a professor at MIT and the founding director of Cybersecurity at MIT Sloan Consortium. The first step is to identify exactly what in the process needs to be protected. The idea is to identify unacceptable losses and the key risks that could lead to them.

Unfortunately, this exercise is not one that most companies do on a regular basis. “When you ask what are the most important functions in your business are, most executives stumble around, trying to think that through clearly,” reports Madnick. “And if they give you an answer, they often change their minds in retrospect.” Consequently, he stresses the need for taking the time up front to carefully identify what needs to be protected.

Once a company performs this exercise, the second step in MIT’s cybersafety method is to develop a model of who or what controls the activities that occur at each function. This control hierarchy must include every influence, whether it be mechanical, computerized, or human. Who or what determines the state of the activity at hand? Then, who or what controls that controller? And the questions continue recursively at every supervisory level higher in the control hierarchy, all the way to the executive suite and even beyond to outside regulatory bodies.

Engineers can use this information to execute the third step, which is identifying control actions that could be unsafe, disruptive, or damaging. Here, Madnick says the key is to think about what the process could do, rather than what it is supposed to do. For example, what would happen if a corrupted sensor signal prevented a controller from taking corrective action or caused it to act at the wrong time? What problems would be caused by changing a sign in a variable-speed drive to make the motor run backwards?

The fourth and final step is to hypothesize how controllers could interact to issue unsafe commands, given the malicious actions of an attacker. Analysts can now identify new requirements that would prevent the worst possible outcomes named in step one.

To help with these kinds of studies, some companies are hiring external experts to conduct periodic security audits and threat tests. “This amounts to proactively employing hackers to find potential vulnerabilities that could be exploited by other hackers,” says Horch.

Conduct regular drills

Besides using a top-down analysis to identify risks, another best practice that cybersecurity can borrow from safety programs is to conduct regular drills. The goal here is not so much to train workers for every possible kind of attack, but to establish the necessary mindset. “Most engineers did not study cybersecurity in college, especially if they went to college more than ten years ago,” notes Madnick. “So, it isn’t on their minds.”

He points to the attack that a disgruntled contractor launched against the Maroochy Shire water authority in Australia back in 2000. When the series of sewage spillages and other problems began occurring, the staff just assumed that the incidents were due to a string of bad luck. “They didn’t even consider the possibility that they had been under a cyberattack for three months,” says Madnick. “Unfortunately, that situation still remains true in many manufacturing facilities.”

Regular cyber-incident drills can change that by sensitizing personnel to consider this possibility much earlier. “In a cybersecurity incident, the time that it takes to detect suspicious system behavior or compromise and to respond has a direct relationship to the severity of the impact,” says Tindill.

Drills are also a good way to train the operations staff. Not only are drills an opportunity to practice responding to attacks, they are also effective at transferring knowledge to less experienced staffers. “Your most senior person may not be present when a cyber-incident occurs,” notes Tindill.

Besides drills, he also advocates other measures common in safety initiatives, such as educational seminars, reminders, awareness campaigns, compliance controls, and studying data collected from behavior-based and near-miss reporting.